Automated Anti-Virus Deployment

Michel Leonard, Alessandro Berni, Diego Merani
NATO Undersea Research Centre
Viale S. Bartolomeo 400
19138 La Spezia
Italy

netcentric@saclantc.nato.int

SUMMARY

NATO Undersea Research Centre (SACLANTCEN), the research establishment of the Allied Command Transformation (ACT) strongly relies on Network Centric technologies and capabilities to improve the effectiveness of its scientific research. This requires architectures for the interconnection and data sharing that are flexible, scalable, and built on open standards, to ensure transparent interoperability between shore laboratories (both NATO and national) and assets located at sea (research vessels, buoys, autonomous vehicles, sensors and acquisition systems), all connected using a wide range of communications media (e.g. SATCOM, wireless at-hoc networks, acoustical undersea communications).

In addition, to fulfil its mission, SACLANTCEN has an extensive cooperation program with scientists and researchers, consultants and contractors, civil and military personnel coming from several NATO nations. It is a common requirement for them to be connected to the Intranet and to the external Internet.

During at-sea experiments, and whenever a joint research or partnership requires it, computers coming from several external (national and non- national) networks need to be connected to our network, and be able to exchange and share data sets with staff members' computers. External collaborators and visitors also need to keep in contact with their home laboratories or institutes, using the Internet to exchange e-mails or files.

Staff members make large use of Internet to perform their daily duties. The use of Internet is encouraged to distribute information to enhance SACLANTCEN business and visibility; the unclassified network, for this reason, is heavily used to exchange data with external world through Mail, HTTP, FTP transfers. Also the use of Internet is necessary to download security patches for CIS systems, and allows the automatic update of anti-virus signatures.

1.0 THE THREATS

The number of computer viruses in the world follows an exponential growth. From two dozen in 1989, 6000 in 1995, it reaches more than 85.000+ viruses in the wild today. According to tabloid press, 50 percent of all emails could contain a virus in 2014.

In 2003 alone, virus attacks cost global businesses an estimated 55 billion dollars in damages. This represents a substantial increase compared to the roughly 25 and 13 billion recorded respectively in 2002 and 2001.

Paper presented at the RTO IST Symposium on "Adaptive Defence in Unclassified Networks", held in Toulouse, France, 19 - 20 April 2004, and published in RTO-MP-IST-041.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **01 NOV 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Automated Anti-Virus Deployment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NATO Undersea Research Centre Viale S. Bartolomeo 400 19138 La Spezia Italy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001845, Adaptive Defence in Unclassified Networks (La defense adaptative pour les reseaux non classifies)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**25**	

The term “malicious code” is used to refer to all code produced with malicious intent, including viruses, Trojan Horses, and worms. Viruses are accounted for the vast majority of malicious codes. Therefore, the term “virus” and “malicious code” will be used interchangeably in this document.

Viruses will not go away anytime soon. A recent CSI/FBI survey indicated that about 98% of respondents have implemented anti-virus software as a security measure. Nevertheless, every day the destructiveness of viruses reach new heights and highlight how primary methods of dealing with viruses today simply aren’t working well enough.

Laptops, wireless devices, file sharing and user behaviour contribute to an ever-expanding set of infection points, leaving companies scrambling to secure their networks. However, history has shown that proactive companies, following a handful of essential security practices fight better against malicious code exploits. These controls include protections such as anti-virus tools, virus walls, specific configuration for routers, email clients, email servers, Web browsers, and security applications that are generally easy to implement, require infrequent updates, and go unnoticed by the average user because of their transparency.

The NATO Undersea Research Centre (NURC) records more than three million high-risk rated attempt of attacks each year. Firewalls are constantly under attack. At least half a dozen of perspicacious and motivated hackers are conscientiously scanning for possible vulnerabilities. However, the biggest threats and fears are concentrated in a few viruses among the 50.000 knocking at the Center doors every year.

Since 2001, the Centre has taken a proactive and adaptive stance in securing its networks. The anti-virus strategy is no longer deployed as stand-alone applications. Rather, it is a layered defence system deployed with other components like host or network-based intrusion detection, global and personal firewalls, logical network security, forensic analyser, etc. By melding these disparate technologies, heterogeneous mechanisms are combined to effectively protect the Centre against new and unknown threats. Even though a few viruses have occasionally entered the NURC network, overall the strategy outlined in this article is until now a success: no payload has ever been successfully activated. The various threats hitting are still transparent to the users’ community.

2.0 THE VULNERABILITIES

Vulnerability is a weakness in processes, administration or technology that can be exploited to compromise IT security. The Vulnerability of our computing architecture has increased with the convergence of several technical factors. The homogeneity of computing hardware, operating systems, application-software and communication platforms is a major enabler for computer viruses, worms and Trojan horses. Together with the increasing connectivity and growing amount of today’s communication systems, it permits viruses to spread faster, and to a larger target audience. The latter are easily built using omnipresent application-specific (e.g. macro languages) or high-level programming languages. Finally, the migration of the PC from the corporation to the home, and the further adoption of home networking have lowered the bar for virus development.

During the last twenty-five years, computer viruses have evolved from a single computer program capable of local infection to complex software worms able to shutdown and damage entire networks. The evolution combines all new technologies. Today, “blended” or “convergence” threats use network viruses, spam as a vehicle, and social engineering as a lure.

Blended threats typically use multiple mechanisms to spread, combining traditional hacker techniques to find operating system or software vulnerabilities with virus-like behaviour to spread further and cause damages. Blended threats include hacker-like behaviour to automatically probe for and exploit system vulnerabilities. Once the vulnerability is found, the worm can remotely infect the computer and data accessed. It can also be used as a proxy machine for mounting further attacks or even distribute spam emails. Once inside the internal network, it will spread like wildfire.

In the future, viruses will be able to carry multiple intelligent payloads residing only in RAM and firing four or five different actions on a target. A single virus will be capable of entering a network, paralyse or cripple the network infrastructure and its equipment, perform intelligence by monitoring the traffic during the recovery, and “a la carte” alter the confidentiality, integrity or availability of the target architecture.

Social and cultural aspects have also had an impact on present and future vulnerabilities. The Internet is carrying the seeds of a new culture characterized by the universal and instantaneous access to information. Malicious source codes, virus generator kit and vulnerabilities are accessible at anytime, by anybody and from anywhere in the world. With very limited knowledge, it takes only a few minutes to create variants of dangerous viruses and infect thousands of computers. The human factor is the weakest link in the security chain of an organization. Viruses target this vulnerability by using social engineering, which is the art and science of getting people to comply with specific wishes. Apart from security awareness, there is no effective way to protect against such techniques. Indeed, no matter what security measures are implemented, there will always be the possibility of influencing the “human factor” by social or cultural events. The “I love you” virus is one of the most famous examples.

The dependence of defence systems on external or commercial companies creates indirect vulnerabilities. Even if heuristic features (rule-based techniques allowing to discover unknown viruses) give good results (more than 50% detection for unknown binary and more than 80% for unknown macro virus), the detection of a new virus solely depends on the goodwill of anti-virus companies. For example, some companies do not include new viruses in the detection list until a threat level trigger is reached. Repeated apparitions of new virus variants in a very short time often weaken detection and deletion engine updates. For example, on a particular brand, recent events of various MyDoom virus versions have led to CPU Denial of Service. With the exception of the Eicar signature, there is no way to assess the efficiency of an anti-virus. Like for any security system, there is nearly a forced blind trust.

While building or updating security architecture, it will be important to understand the cocktail of techniques that will be used by a virus’ creator. “Day zero attacks” (attacks that occur before countermeasures are available) are expected to increase to reach 30 percent in 2006 compared to 15 percent in 2003. A proactive strategy must, therefore, be able to prevent, confine and cure the systems of any virus.

3.0 THE RISKS

The risk to an organization like NATO is the product of threats and vulnerabilities. Risks associated to classified information are obvious. Comparatively, risks to NATO unclassified information and networks are initially less obvious. Threats comes across a large spectrum of diverse activities ranging from non-NATO state sponsored information warfare and espionage, commercial intelligence, investigative journalists, single subject pressure groups (e.g. alter-mondialist, peace organization, whales defenders, anarchists, etc), malicious code writers, hackers in quest of glory and misuses of the organization bandwidth or network equipment for various purposes. Correct setups for servers and firewalls forbidding unnecessary inbound or outbound traffic efficiently reduce most of the threats.

As is the case for commercial entities, the greatest damage to NATO unclassified networks comes from the virus and worm’s fraternity. Malicious codes are a direct threat to the core information security objectives (confidentiality, integrity and availability) of any organization’s information assets. Damages can be measured in downtime and costs to recover the situation. The associated costs can be compared to any research facility of a high technology commercial company. However, damages caused by a Trojan horse are difficult to assess.

Generally in NATO, unclassified networks are mostly used to communicate low value information with the external world through the Internet by email, web servers and file transfer. The role of the unclassified network connected for NATO Research Centre is somewhat larger. Unclassified information represents a high percentage all information processed. Internet is used to share information with other research laboratories around the world, perform joint researches or experiments. The content of these networks is of high value for the future of the organization, at least in terms of intellectual property.

The aggregation principle may increase the value of the information stored on unclassified network and thus, the risk. Taken separately, bits of information are unclassified. However, combined together, conceivably it can reach a top-secret level. For example, the target strength of an unidentified submarine is unclassified. However, the value of the information is raised an elevated classification level if sonar frequencies and the class of the submarine can be found somewhere else and correlated.

The beauty of the aggregation principle lies in its silent threat and the power of its consequences. Information can be obtained from independent sources placing the information on unclassified networks or Internet in good faith. This is likely to happen in a scientific environment. “Publish or die” is the motto of most researchers. Indeed, peer revision is a classical measurement of the value of scientific works. A typical unfortunate scenario would include four individuals. A coordinator writing a coordination brief describing the experiment with a new submarine, a researcher publishing its result on the target strength, other publishing results on the sonar technology used and a hacker using a Rootkit Trojan Horse. Taken separately each piece of information collected could, in all good faith, be unclassified high value; together the level is classified. Even if detected, it is nearly impossible to correctly assess the damage if the information is dispersed on different computers.

Even if a high percentage of the information processed by NATO is unclassified, it does not mean that the information is not used to plan, prepare and/or conduct military research and exercises. Although NATO regulations prohibit the direct connection of classified systems to the Internet, there is no policy concerning how and where to treat unclassified information prior to its injection into operational systems, e.g. a tactical decision aid system. By silently altering the integrity of data sets temporary processed or stored on unclassified networks, whether voluntary or involuntary, malicious codes could have the potential to place future military operations at risk.

4.0 THE CONTEXT OF THE NATO UNDERSEA RESEARCH CENTRE.

The NATO Undersea Research Centre, located in La Spezia, Italy, is dedicated to fulfilling NATO's Operational Requirements in undersea warfare science and technology. Its Scientific Programme of Work, currently organized along three main thrust areas (Anti-Submarine Warfare, Mine Countermeasures, and Rapid Environmental Assessment) has resulted during the past 40 years in several scientific and technical contributions that are now part of the set of standard capabilities of all NATO navies.

An interdisciplinary team that covers different disciplines, such as acoustics, oceanography, ocean engineering, real-time processing, and signal processing, performs the execution of the Scientific Programme of Work. Over the past years, a continuously increasing focus has been put on Network-Centric technologies and capabilities, which have emerged as essential tools to enable and improve the effectiveness of its scientific research.

The development of Network-Enabled capabilities in support of undersea research requires architectures for the interconnection and data sharing that are flexible, scalable, and built on open standards. This is essential to ensure transparent interoperability between shore laboratories (both NATO and national) and assets located at sea (research vessels, buoys, autonomous vehicles, sensors and acquisition systems). Also, a wide range of communications media needs to be supported (e.g. SATCOM, wireless at-hoc networks, acoustical undersea communications).

The efforts in the development of Network-Enabled concepts are specifically oriented towards the definition of new generations of scientific instruments. The network will be used to improve the transmission of data from sensors to processors, increasing the capabilities of individual instruments. The resulting increase in efficiency will be larger than the sum of the individual instruments efficiencies.

5.0 THE NEED FOR ADAPTIVE NETWORK SECURITY

The unclassified network of the Centre is connected to the Internet, and provides the standard services that are requested to a modern enterprise network: office automation, e-mail, Internet access and workgroup file sharing.

The Centre has an extensive cooperation program with scientists and researchers, consultants and contractors, civilian and military personnel visiting the Centre for periods of limited duration. To enable efficient collaboration, various services are offered on demand to visitors: access to the Internet, file exchange, printing facilities and use of e-mail. These services are provided on land and at sea on both NATO only owned ships (NRV Alliance and CRV Leonardo). The Centre provides connection to the Internet through its own network or part of it as shown in figure 1. The internal network infrastructure has been designed to prototype the development of network-enhanced capabilities.

Guest computers connected to the internal network introduce additional threats. Either downloaded or already active on guest hosts, malicious codes represent a wide range of threats able to use the network infrastructure as an infection vehicle. For example, in a Microsoft-based network, a virus spreading through shared directories can infect all systems in a few minutes. Policies are able to mitigate, partially, the risks. However, when prevention fails it is needed to detect and confine immediately the danger. Identifying and removing the origin of an internal attack will always be challenge.

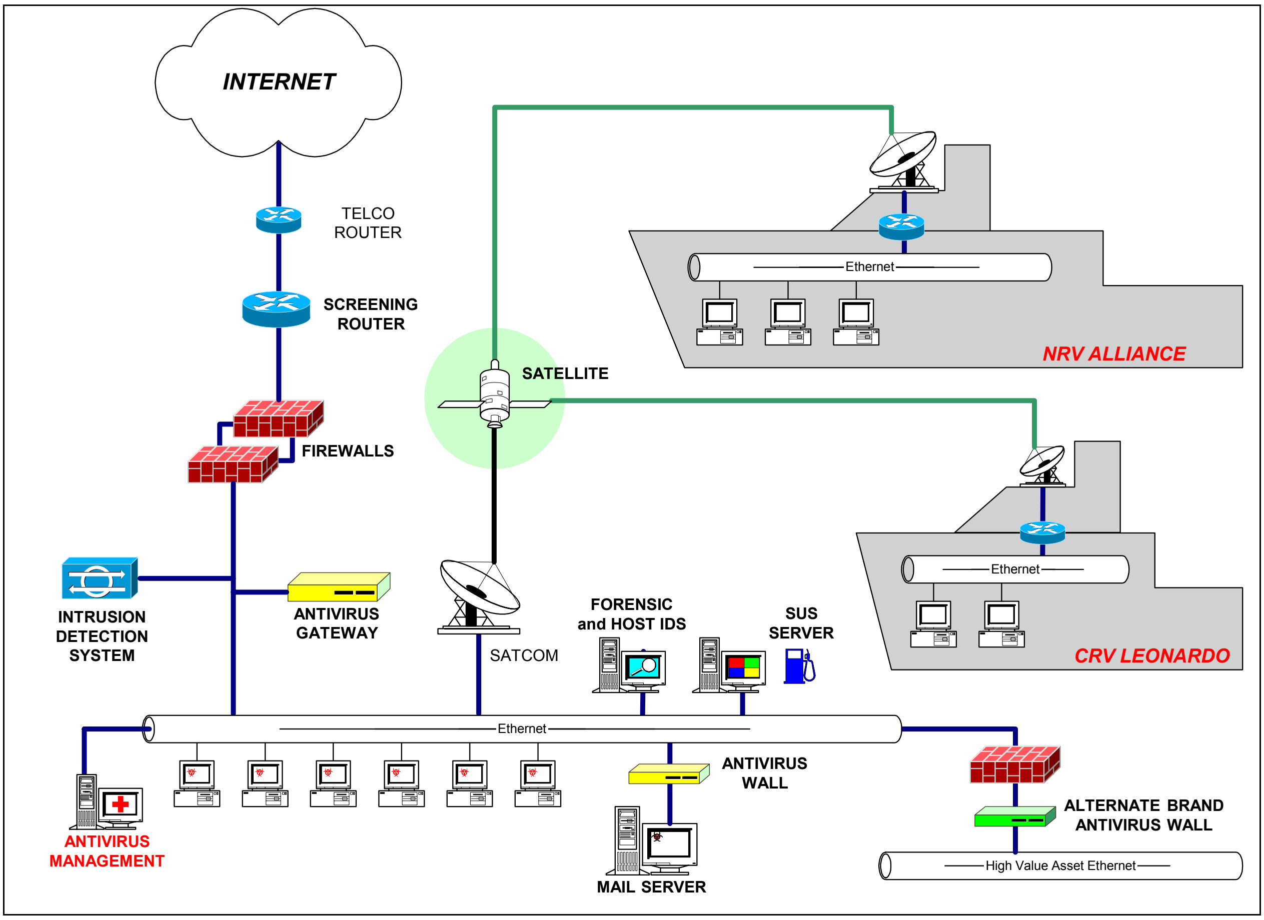


Figure 1 - Standard NURC Unclassified network structure

Malicious code writers have achieved a state of the art where their most complex creations take days or weeks to analyse and develop countermeasures for. However, the average computer virus can be processed in minutes. Virus technologies will continue to co-evolve with the virus technology. The war is in the leap time between the treat and the cure. Unfortunately, threats will always have a step ahead.

The NURC network architecture is modified in a substantial way roughly 30 times in a year to fulfil the requirements of scientific experiments. At each time, complex setups involving satellite communications between multiple ships, inside guest networks, asymmetric networks increase the risk of vulnerabilities from the inside or the outside world. There is a need for continuous vulnerability management. At any time, exposures must be discovered, prioritised, shielded and mitigated. Security controls must be established and enforced. Once root causes are eliminated, Science must go on.

6.0 NURC STRATEGY

The sooner an infection is detected, the lower the cost of eradicating it and the lower the residual costs due to damage and data loss. The most effective enterprise security strategy is preventing attacks by selecting, developing, deploying and maintaining systems that eliminate or shield vulnerabilities. The centre efforts on prevention reflect clearly this statement. However, in a scientific environment the sinews of the war is to find an acceptable compromise between scientific and security requirements.

6.1 Standard Anti-virus Technologies

Standard Anti-virus technologies are the core of the Centre's automated Anti-virus deployment systems. Its purpose is basically to protect all assets from known malicious attacks by multiple protections in series. It is also designed to keep up with new sets of malicious code risks created by the pervasive adoption and use of web service and active content.

Malicious code writers have achieved a state of the art where their most complex creations take days or weeks to analyse and develop cure for. During the last years, repeated updates in very short times have led several times to defective scanning engines leaving networks without any protection. The Centre's layered defence approach is a direct consequence of these incidents. Each protection is a self-sufficient layer able to fully protect a network. To reach a target, a virus must pass through at least three different protections belonging to at least two different vendors. Beyond redundancy, it turns the competition between the vendors to good account to optimise response times in terms of signature availability, signature delivery and systems reliability.

The Centre's automated Anti-virus deployment is mainly composed of virus-walls (also called anti-virus gateways) and local anti-virus systems.

Anti-virus software is installed on every computer connected to a network. It protects any server or desktop against viruses, vandals, worms, Trojans and other types of malware. Signature-based scanning, heuristic analysis, generic detection, generic decryption and behavioural analysis are available and enforced each time a file is read or written. In combination, these methodologies detect not only all known viruses in the wild, but also malicious Java, activeX and Java Applets, as well as polymorphic viruses, worms, Trojan Horses, Zombie Codes and other security threats.

A central management software solution enables security administrators to manage and enforce anti-virus policies transparently. Virus definition databases are transparently and automatically updated one or two times per day with minimum bandwidth use. It can be configured to enforce updates or upgrades to selectively to one or all of users in order rapidly to stop an outbreak. The standard Centre policy calls for a full scan of all desktops every day.

A Virus-wall or virus-gateway is a dedicated appliance installed at every entry (gateway) of a network. It scans email and Internet content before it reaches the network. Upon live receipt of signatures, it delivers instant gateway security on SMTP, HTTP, FTP, and POP3 traffic. Heuristic searches and generic protection are activated on both inbound and outbound traffic. Once a virus-wall is updated, local anti-virus software are updated with minimum bandwidth and disturbance for users. When a network entry defines the boundary between two internal networks, for example between a low value network and a high value network, another vendor product is used. In addition, for sensible servers, like email servers, are protected with a virus-wall mounted in pass-through (transparent) mode.

The layered defence approach protects gateways, e-mail servers and computers. An inbound virus needs to defeat first the network virus gateway, second pass through the e-mail server virus-wall and third beat all local anti-virus software. Early in March 2004, the first two levels of protection have failed due to vendor's mistakes. Fortunately, the third level protection reacted correctly. For traditional viruses spreading by email, the layered defence system works also very well for virus entering via a media. It first needs to beat the local anti-virus, second defeat the server virus wall and third pass through the virus gateway to spread to the Internet or an internal high value network.

New viruses are able to bypass gateway level web and email virus protection spreading through other channels. Firewalls are adjusted to reduce additional threats. They are used to secure these ports and minimize the number of ports opened. Any inbound or outbound port outside the scope of a virus-wall is strictly controlled. Authorization to use the port is granted on a case-by-case basis. If granted, it is only for a limited period and additional protection measures are taken to reduce the potential threats. Several additional protections are implemented on firewalls or screening routers (e.g. time-based services) but those fall outside the scope of this article and its classification.

Anti-Spam Appliances detect spam (unsolicited e-mails) at the gateway, preventing it from consuming valuable network resources. Spam is stopped cold through advanced, rules-based scanning and scoring plus multiple levels of intelligent spam detection. Although Anti-Spam Appliances contribute little to the global anti-virus strategy, they reduce potential threats related to malicious codes using Spam as a spreading vehicle.

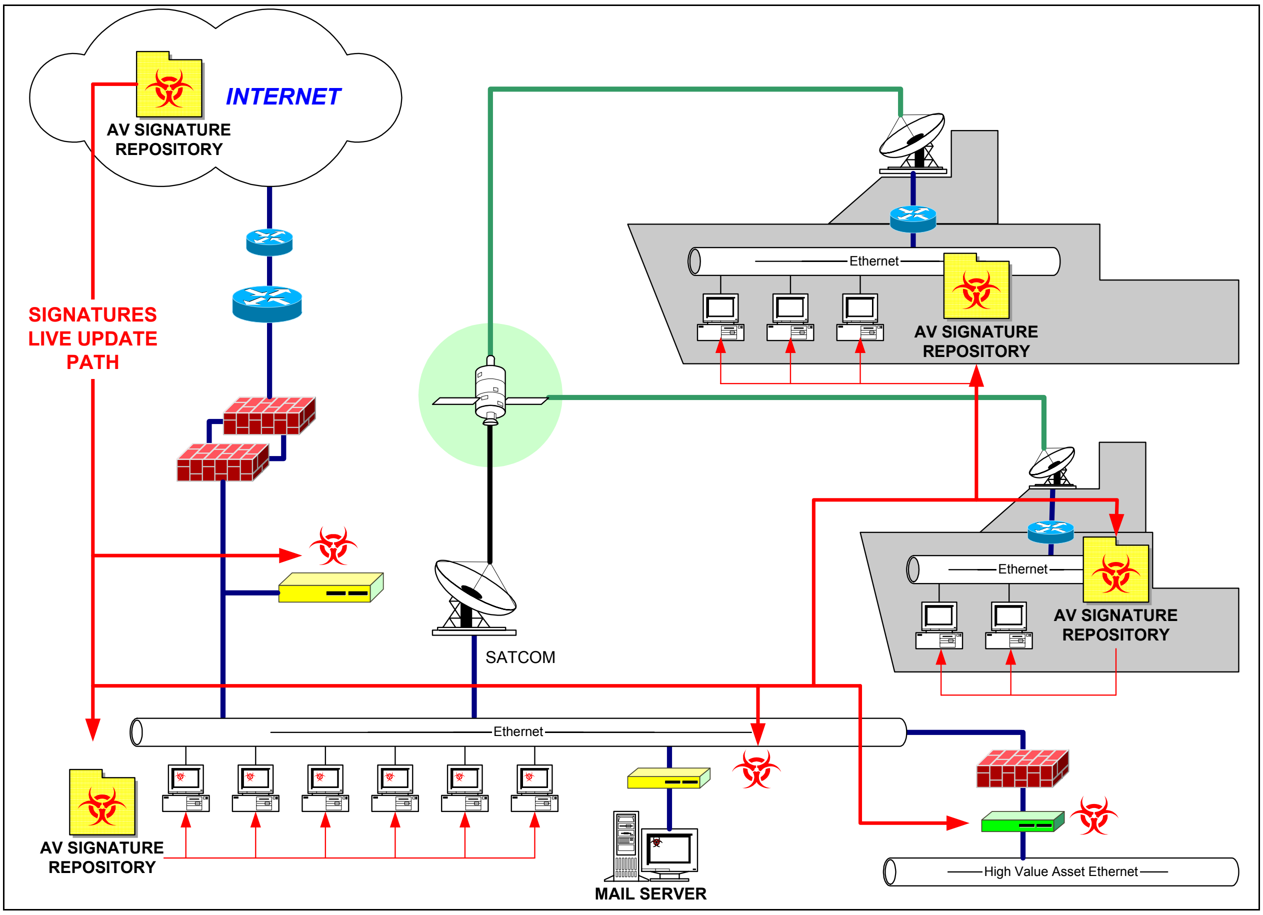


Figure 2 – Automated Anti-Virus deployment (layered defence system).

One of the major weaknesses of this layered defence approach resides in the usage and potential threats created by laptops. Nothing prevents a user with an infected laptop to connect to a network and spread a virus like a tsunami. However, Network Admission Control is the next technology to be implemented in the Centre (e.g. Cisco Network Admission Control – CNAC). This interesting and a long awaited technology is now emerging slowly on the market. It should automatically limit network access from unprotected assets. It is the link between the anti-virus technology and the network technology. Prior to any connection to a network, the security level of a computer will be systematically assessed and accepted by the network security management system.

In the mean time, a strict security policy is enforced. A policy is as necessary to good information security program as a solid foundation is to a house. Policies, standards, and guidelines form the foundation of any information security program. Recently, all Centre's Communication and Information Systems (CIS) policies have been updated to take into account the technological evolution of information technologies and its threats. A Security Authority must approve every change on networks or systems. Firewalls, anti-virus gateway, Intrusion Detection System (IDS) are mandatory on any entry point of a network. An up-to-date anti-virus is mandatory on every computer. Failure to comply with these regulations can have severe consequences. Security inspections are conducted by Centre's security officers on regularly and randomly bases.

6.2 Complementary Technologies

The previous section showed how the centre strategy is able to block known inbound viruses and known email spreading viruses infecting an internal network. What about blended threats entering the network by other means? The potential number and frequency of malicious-software signature will increase exponentially with the emergence of active content, web services (XML, SOAP, .NET), and peer-to-peer technologies. Together with the increasing complexity, it will contribute to double the number of "day zero" attacks. How to prevent disasters caused by a "day zero" attack? Complementary technologies must be used to better prevent, detect and confine unknown threats.

Prevention against unknown threats is targeted to reduce vulnerabilities. Several technologies can reduce in a substantial ways the vulnerabilities and thus the threats for the centre.

The Centre vulnerability management strategy includes active vulnerability and compliance monitoring, as well as well-defined response processes. Each change in the environment could introduce a new vulnerability, and new external threats are constantly emerging. Therefore, the Centre performs frequent vulnerability scanning to minimize the number of unknown exposures both on firewalls and on desktop platforms.

Most viruses are today targeted to Microsoft applications and operating systems. Therefore, every Microsoft operated computer is updated every night with the latest patches by means of Service Update Server (SUS) receiving live updates directly from Microsoft. In addition, Microsoft security policies are used to thwart malicious codes on high value system by locking down all PC to only allow trusted software to be executed.

Heuristic analysis is only able to discover more than 50 percent of unknown binaries and 80 percent of unknown Macro viruses. Several technologies are needed to confine and detect the rest of the threats. These are particularly required to track potential one-of-a-kind malicious codes targeted to alter the confidentiality or the integrity of NATO information.

Virtual Local Area Networks (VLANs) are used to confine malicious codes or malicious network activities once detected. VLAN's were initially formed to group related users regardless of the physical connections of their hosts to the network. Although switch designers had something other than security in mind, VLANs make it possible to isolate traffic that share the same switch, or even group of switches. This technique is called partition and is used in the Centre to enforce need to know policies. Each computer must be authorized to enter in a VLAN. In case of problems, a complete VLAN or a single computer can be isolated in a few seconds manually or automatically.

Several Network based Intrusion Detection System (N-IDS) monitors all traffic passing on sensible segments where a detector/sensor is installed, reacting to suspicious anomaly or signature based activity. As well as alerting to an attack, the N-IDS can automatically defend against them. This is achieved by reconfiguring switches/routers to reject from the objectionable sources (shunning) or by crafting some packet to reset the connection. If needed a N-IDS is able to shun traffic using routers' Access Control Lists to isolate malicious activities. Next generation of IDS will be able to shun on virtual interfaces, thus increasing the effectiveness of the actions also inside a VLAN enabled environment. N-IDS Signatures are updated through live updates.

A central Host based Intrusion Detection System (H-IDS) collects all audit trails recorded on each computer. It monitors all event logs for suspicious activities. The H-IDS is the best placed to detect malicious code emerging from the inside of the network as well as those who have infiltrated the network by evading all other methods of detection. The H-IDS includes signature analysis across multiple events and/or time. It also incorporates heuristics analysis to detect unknown malicious behaviours.

Working with IDS is a complex task. Indeed, IDS systems require a substantial amount of attention, training and fine tunings to reduce false (positive) alarms. Therefore, IDS systems are mostly used as passive systems. The centre H-IDS is almost always used as a passive system; it detects a potential security breach, logs the information and signals an alert. The N-IDS is mostly used as a passive system. However, when required it is used as a reactive system that responds to suspicious activities by shunning switches to block network traffic from the suspected malicious source. H-IDS and N-IDS are valuable tools to detect Trojan Horses. For example, the N-IDS is able to detect covert activities like back tunnelling activities.

Last but not least, the most complex tool of the NURC security program is a very complete and powerful forensic analyser. It can be thought of as a pumped-up protocol analyser combined with sophisticated analysis and data-visualization tools. It gathers data about a network, its structure, its traffic and its users by analysing raw network packets. Raw packets are assembled and organized into a knowledgebase and render events into visual representation. The program can combine logs from firewalls, routers, or intrusion-detection systems with saved session information for comprehensive analysis of network activity and enables the examination of real-time suspicious activities. The program contains a collection of advanced tools for creating and examining image representation of network traffic through advanced visualization of logical, physical or topological view of a network. This software is a major asset to detect possible one-of-a-kind malicious code and especially intelligence related Trojan Horses. Unfortunately, this strategy falls outside the scope of this article and its classification.

7.0 CONCLUSION

Since 2001, the NATO Undersea Research Centre has taken a proactive and adaptive stance in securing its networks. The strategy is constantly reviewed and adapted to fight the development of increasingly powerful, more complex computer virus threats. By continuously anticipating the next step in the co-evolution of the virus technology and incorporating countermeasure, this adaptive approach has been, until now, a true success. However, the war is far from being over . .

Acknowledgements

The authors would like thank Mr Jim Obal (SACT INFOSEC) and COW3 David Olson (NURC) for their valuable comments.

8.0 BIBLIOGRAPHY

[1] “Commentary”, M. Nicolett, Gartner Group Research Note COM-20-7278 – 3 September 2003.

[2] “Management update: Increase security in Desktop Computing Through Diversity”, R. Wagner and J. Pescatore, Article IGG-10152003-03, 15 October 2003.

[3] “Microsoft offers MyDoom Reward”, Andrew Stein, posted in money.cnn.com, 30 January 2004

[4] “The Global Threat To information Technology Security”, posted in Itsecurity.com, 14 April 2003.

[5] “The Evolving Virus Threat”, Carey Nachenberg, Symantec Corporation, posted in Symantec.com.

[6] “Blended threats-How to combat them” – White paper – posted in datafellows.com , F-secure Corporation, December 2003.

[7] “Intrusion Detection Terminologies (part one)”, Andy Cuff, posted in securityfocus.com, 3 September 2003

[8] “Intrusion Detection Terminologies (part two)”, Andy Cuff, posted in securityfocus.com, 24 September 2003

[9] “Dynamic Virtual LANs for adaptive network security”, Diego Merani, Alessandro Berni, Michel Leonard, *in* RTO IST-041/RSY-013 Symposium on “Adaptive Defence in Unclassified Networks”, Toulouse, France, April, 2004

[10] Berni A., Leonard M., “Antisubmarine Warfare wireless network for real time data fusion”, Proceedings of NATO Regional Conference on Military Communications and Information Systems 2001, Zegrze, Poland, 2001

[11] Berni A., Leonard M., “Antisubmarine Warfare wireless network for real time data fusion”, RTO Meeting Proceedings RTO-MP-065 - AC/323(IST-023)TP/12 , Military Communications, Warsaw, Poland, 2001

[12] Leonard, M., Berni, A., Merani, D., “Architectures for Network Centric operations in undersea research” RTO SCI-137 Symposium on “Architecture for Network-Centric Operations”, Athens, Greece, 2003

Automated Anti-Virus Deployment

Michel Leonard

NATO Undersea Research Centre

The Need for Security

- Information Warfare and espionage
- Commercial Intelligence
- Investigative Journalists
- Pressure Groups
- Hackers and Malicious code witers

Viruses

Generic term for malicious codes like:

Viruses

Trojan Horses

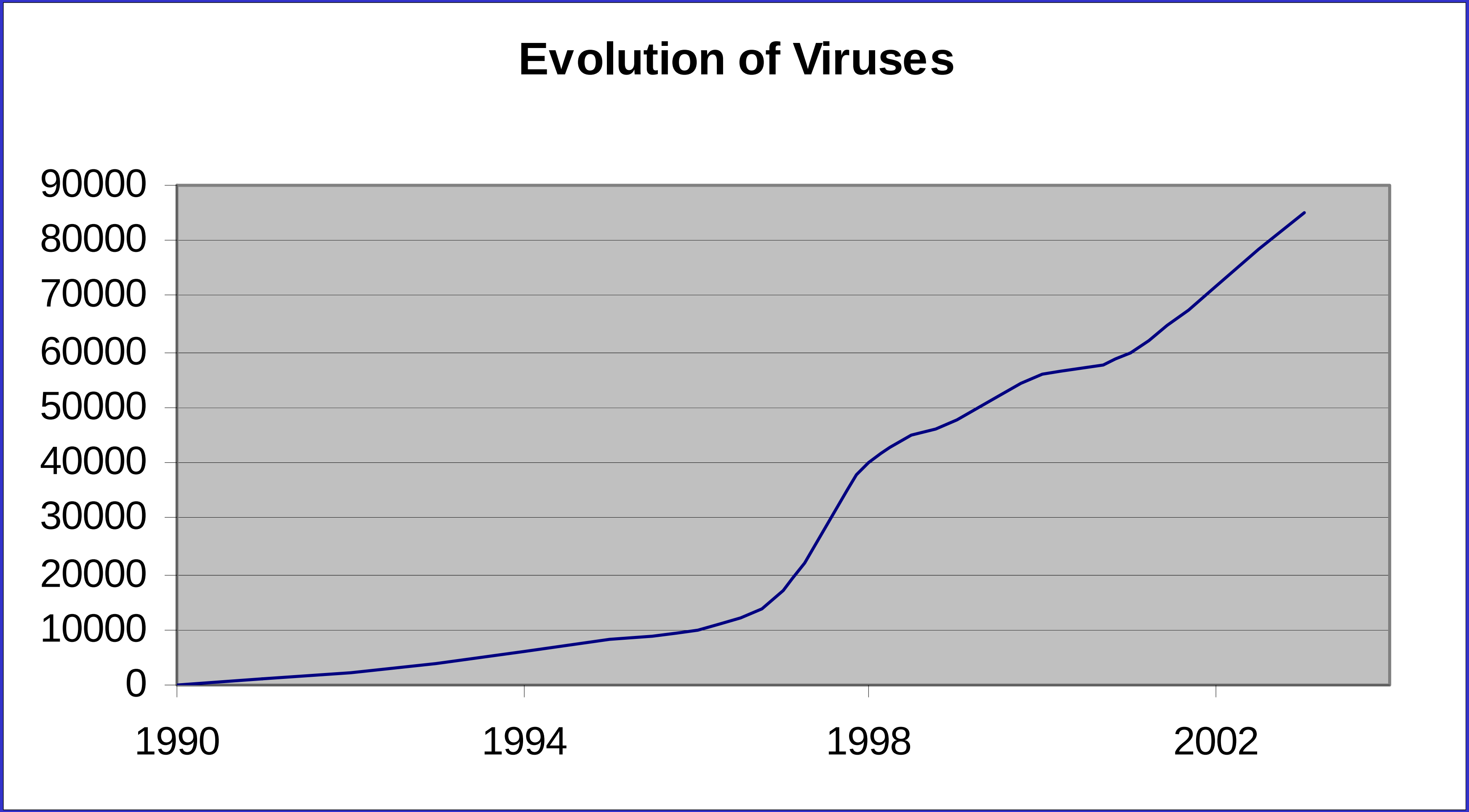
Worms

Zombies

Hoax

…

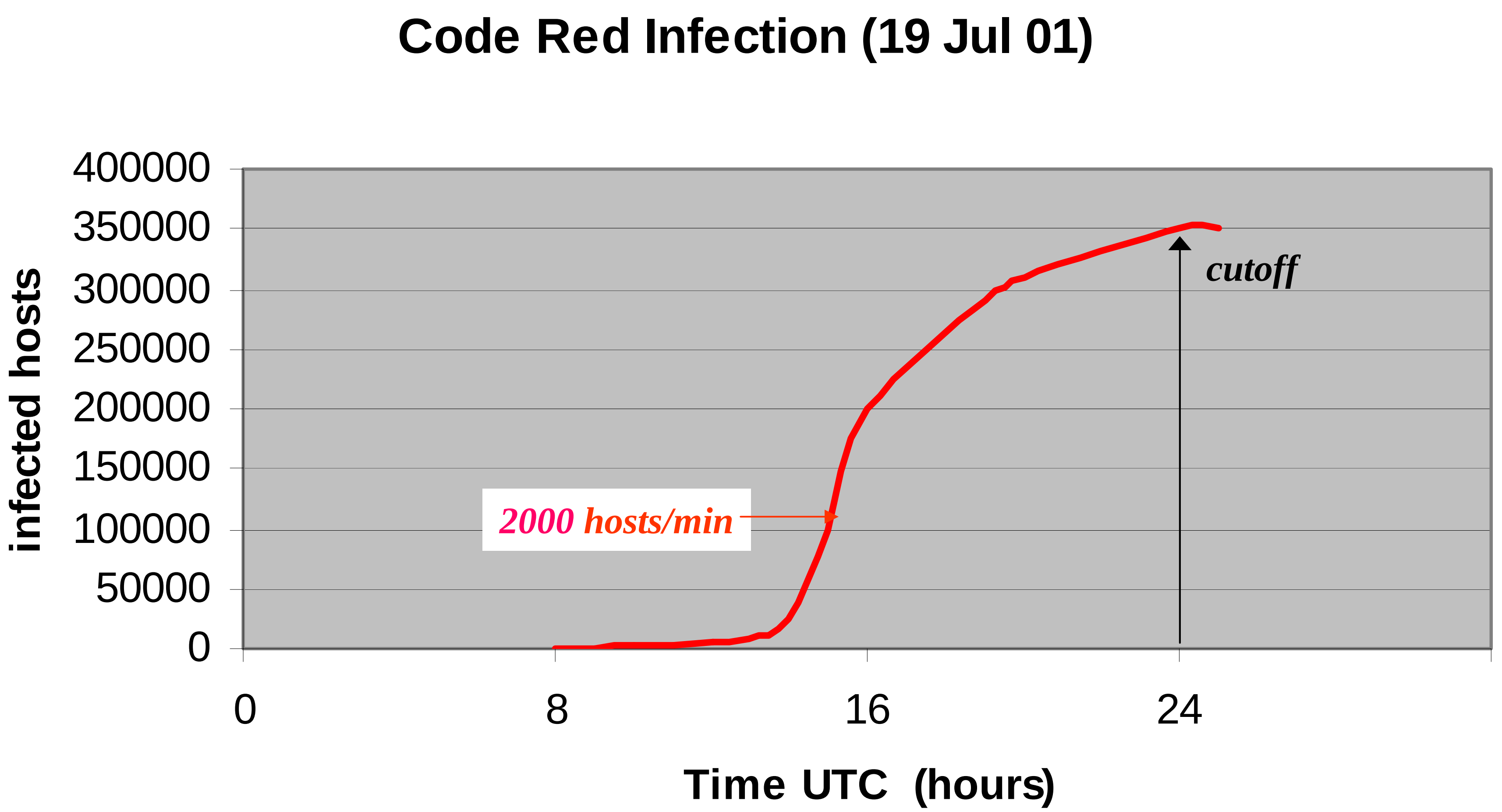
The progression of Viruses



The Threats

- Co-evolution with anti-virus system
- Increasing number of viruses in the wild
- Increasing complexity
- Increasing infection speed
- Increasing damage capacities

Code Red: The wake-up



The Vulnerabilities

- Homogeneity
- Increasing Connectivity
- Omnipresence of HL languages
- Adoption of home networking
- Legacy and weak codes.
- Social Engineering
- External dependence

The Risks for NATO NU

For NATO unclassified networks:

- Availability (increasing importance)
- Confidentiality (aggregation principle)
- Integrity (potential risk of grave dangers)

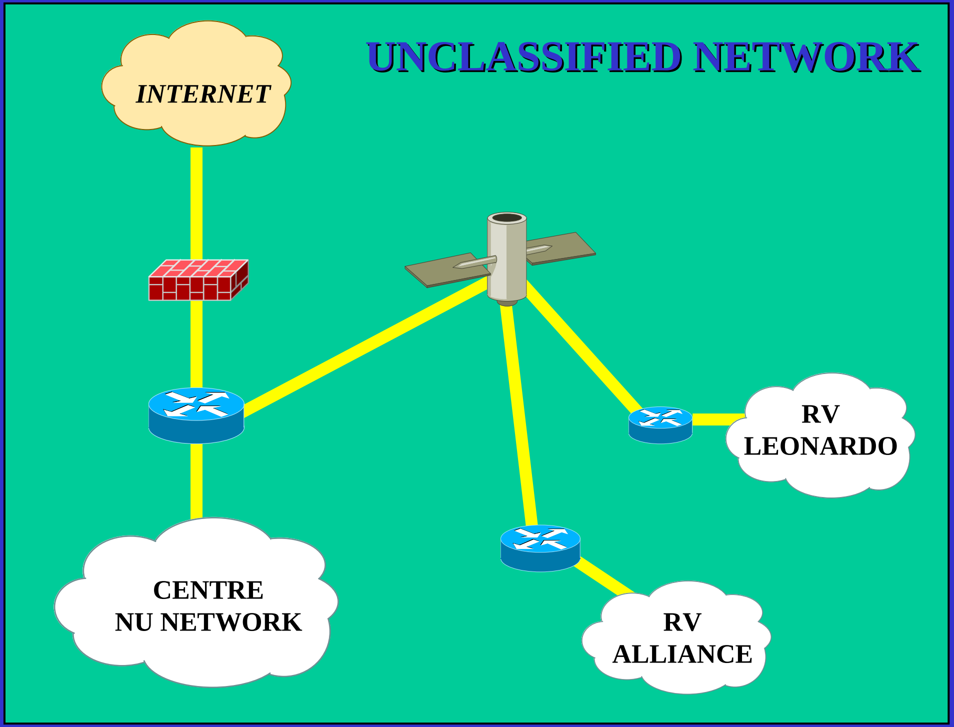
Undersea Research Centre

Mission:

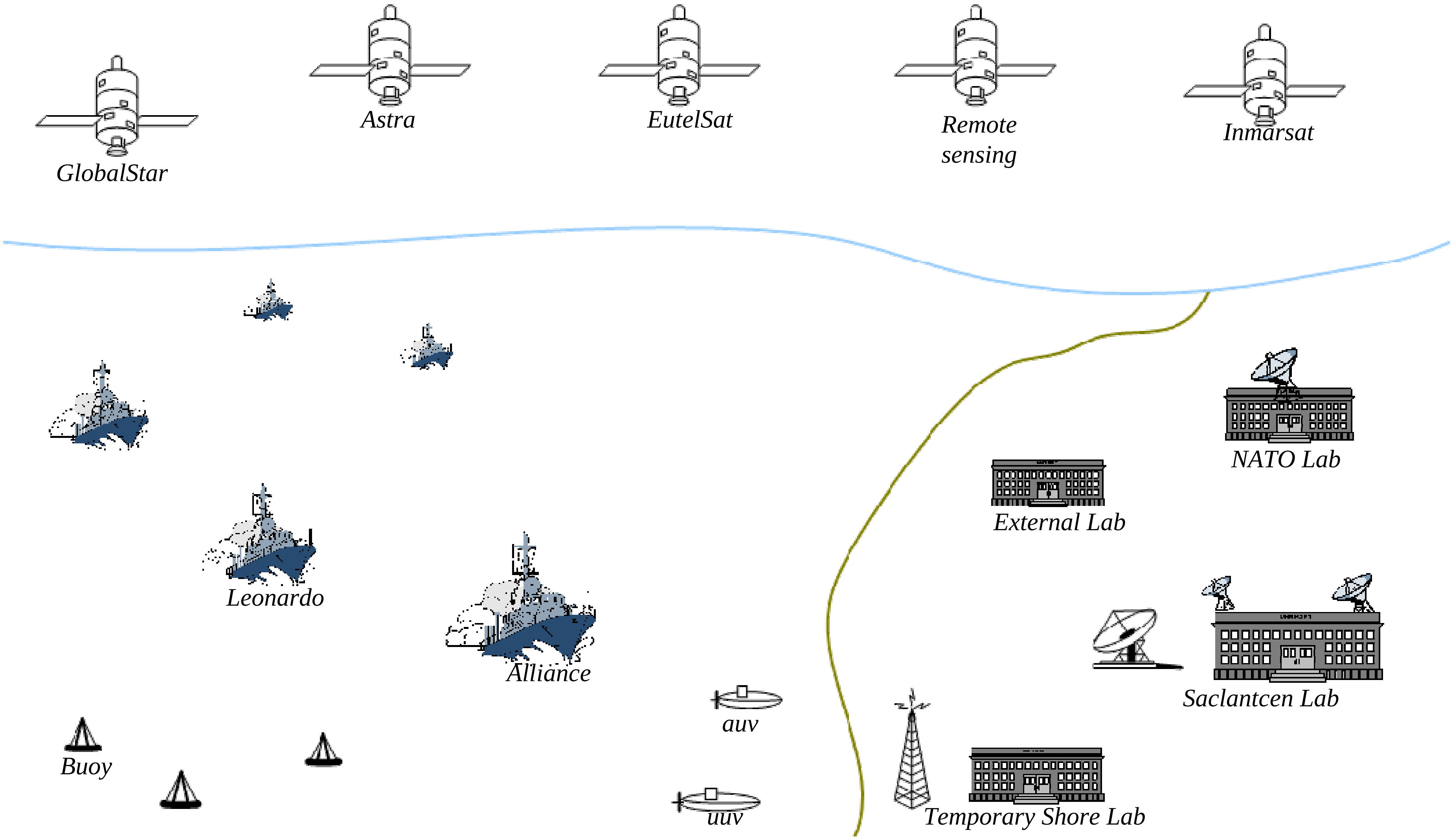
Research in
ASW - MCM - REA
Command &
Operation Support

Resources:

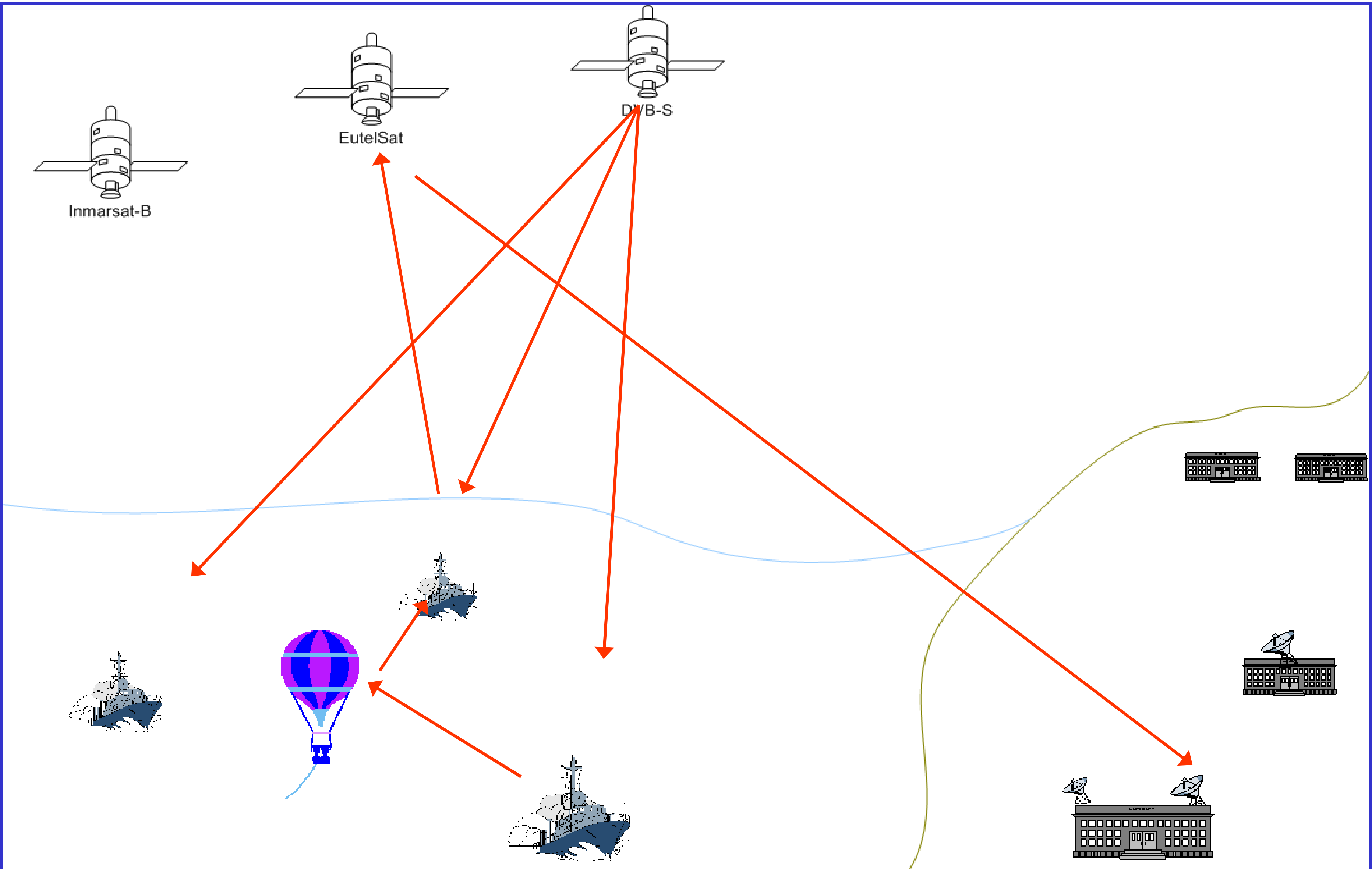
2 Research vessels
Advanced facilities



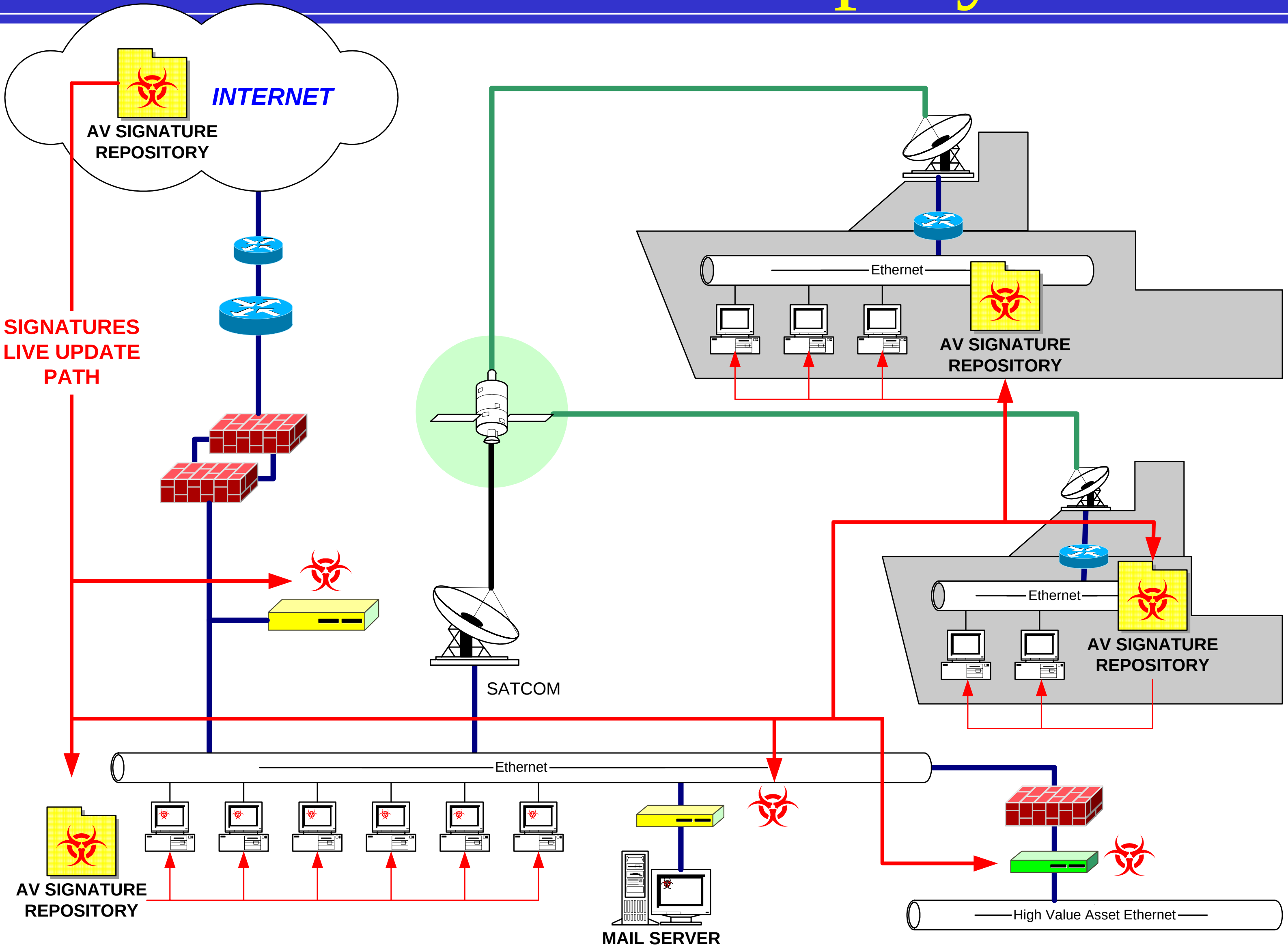
The NURC context



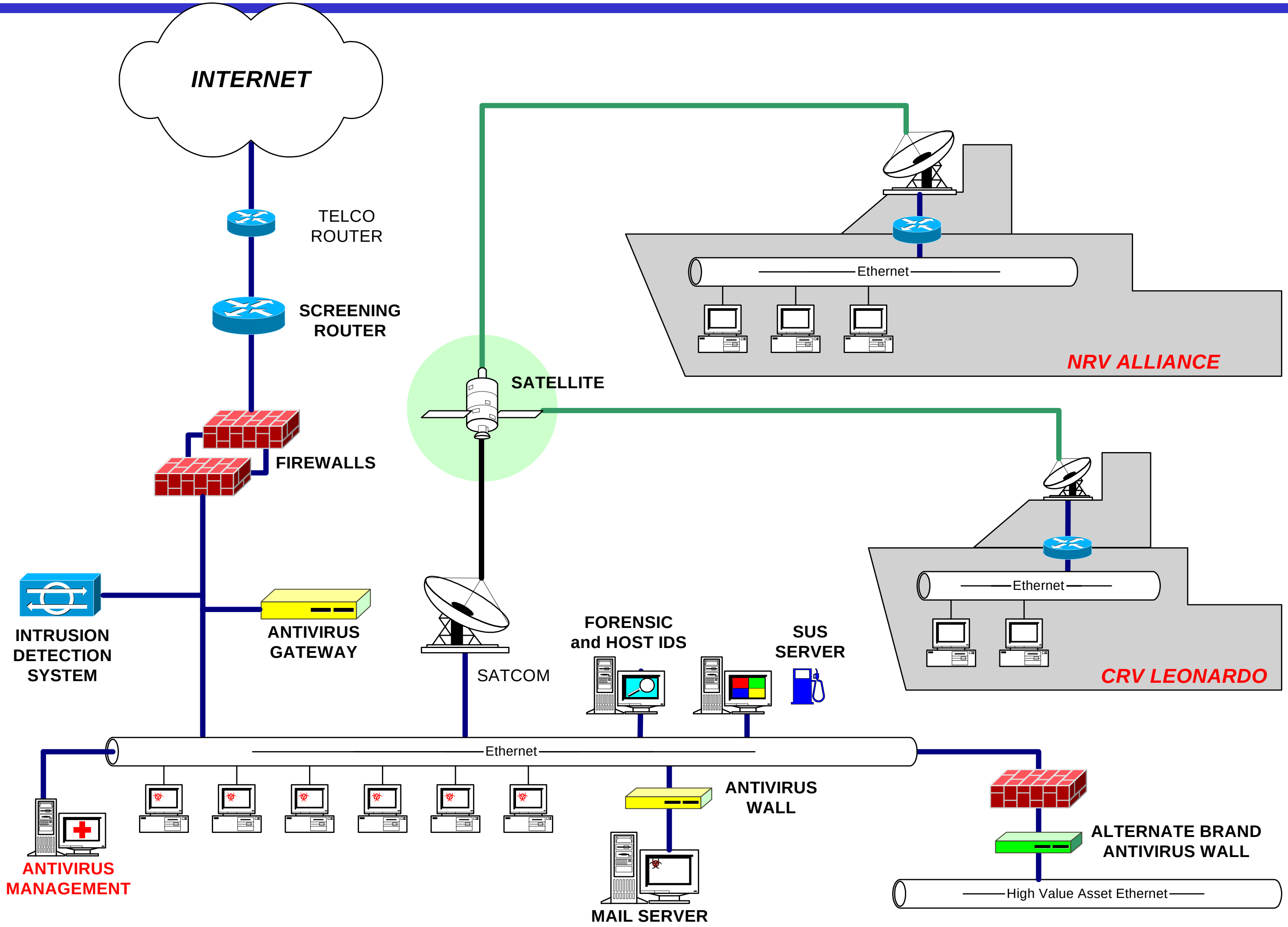
Asymmetric Network



Automated AV Deployment



Adaptive Network Security


INTERNET
TELCO ROUTER
SCREENING ROUTER
FIREWALLS
SATELLITE
Ethernet
NRV ALLIANCE
Ethernet
CRV LEONARDO
INTRUSION DETECTION SYSTEM
ANTIVIRUS GATEWAY
SATCOM
FORENSIC and HOST IDS
SUS SERVER
Ethernet
ANTIVIRUS WALL
ANTIVIRUS MANAGEMENT
MAIL SERVER
ALTERNATE BRAND ANTIVIRUS WALL
High Value Asset Ethernet